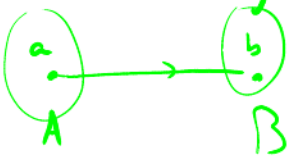
Last Time: Relations

Recall: A relation $A \xrightarrow{R} B$ is a subset $R \subseteq A \times B$.

NB: We built diagrams for relations



iff $(a,b) \in R$.

write xRy for $(x,y) \in R$.

Special: relation on a set $R \subseteq S \times S$.

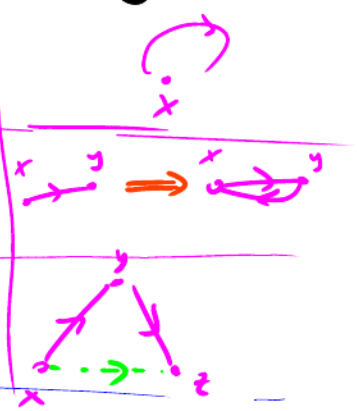
↳ use similar diagrams there (on one copy of S).

Properties a relation on S might (or might not) satisfy:

① Reflexivity: $\forall_{x \in S} [x R x]$

② Symmetry: $\forall_{x,y \in S} [xRy \rightarrow yRx]$

③ Transitivity: $\forall_{x,y,z \in S} [(xRy \wedge yRz) \rightarrow xRz]$



Exercise: For each subset $P \subseteq \{\text{reflexive}, \text{symmetric}, \text{transitive}\}$, either build a relation on a set S which satisfies exactly the properties in P, or prove no such relation exists.

↳ Ex: For $P = \{\text{reflexive}, \text{transitive}\}$, want: build a relation on some set S which is: ① reflexive, ② transitive, ③ NOT symmetric.

Hints: ① Use the diagrams to visualize

② If an example exists, you need at most 4 elts in S.

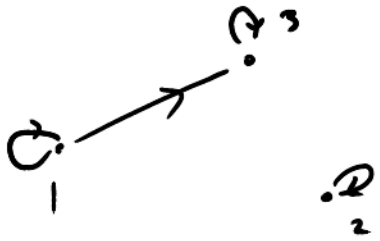
Defn: An equivalence relation is a relation on a set S which is reflexive, symmetric, and transitive.

Ex: The relation depicted by is an equivalence relation. I.E. $S = \{1\}$, $R = \{(1,1)\}$.

Reflexive: duh.
Symmetric: duh.
Transitive: duh.

> All trivial to verify...

Ex: The relation depicted below **is NOT** an equivalence relation.



Not symmetric
($1 R 3$ but $3 \not R 1$)

Ex: Congruence modulo 5 is an equivalence relation on $\mathbb{Z}$.

pf: Recall $x \equiv y \bmod 5$ iff $5 | (x-y)$. ←

Reflexive: Let $x \in \mathbb{Z}$. Now $x - x = 0 = 5 \cdot 0$, and $0 \in \mathbb{Z}$, so $5 | (x-x)$ yields $x \equiv x \bmod 5$. Hence $\equiv$ is reflexive.

Symmetric: Suppose $x, y \in \mathbb{Z}$ satisfy $x \equiv y \bmod 5$. Thus $5 | (x-y)$, so $x - y = 5k$ for some $k \in \mathbb{Z}$ by definition of divisibility. Hence we have

$$y - x = -(x-y) = -5k = 5(-k),$$

so noting $-k \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under subtraction, we see $5 | (y-x)$ by definition of divisibility. Thus $y \equiv x \bmod 5$; hence $\equiv$ is symmetric.

Transitive: Suppose $x, y, z \in \mathbb{Z}$ satisfy $x \equiv y \bmod 5$ and $y \equiv z \bmod 5$. Thus $5 | (x-y)$ and $5 | (y-z)$, so $x - y = 5k$ and $y - z = 5m$ for some $k, m \in \mathbb{Z}$

by definition of divisibility. Hence we compute

$$x - z = (x - y) + (y - z) = 5k + 5m = 5(k+m)$$

and $k+m \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under addition, so $5 \mid (x-z)$, and thus $x \equiv z \bmod 5$. Thus $\equiv$ is transitive.

Hence, $\equiv$ is an equivalence relation by definition (indeed, it is reflexive, symmetric, and transitive). ☑

Remark: If we replace each 5 above by n, we will have the bones of a proof that $\equiv \bmod n$ is an equivalence relation on $\mathbb{Z}$. ☺

NB: Equivalence relations are a useful mathematical tool. They crop up everywhere in maths and computer science...

Functions

Idea: A function is (roughly) an association table: it associates each input of a set S w/ a unique output. → exactly one

Defn: A function from S to T is a relation $S \xrightarrow{f} T$ such that every element of S is related to a unique element of T.

Ex: The relation below is a function:

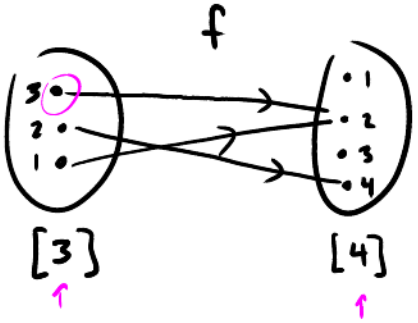


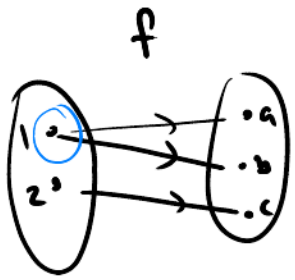
table: ⇝

x	f(x)
1	2
2	4
3	2

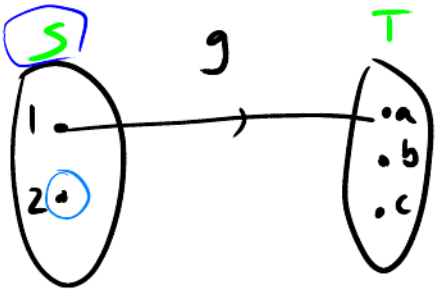
distinct inputs 1, 3 have the same output 2.

(More Complete Definition): A function $f: S \to T$ is a relation w/ every element of S relates to a unique element of T. The domain of f is $\text{dom}(f) = S$ and the codomain of f is $\text{cod}(f) = T$. We say x maps to y when $x f y$. We also write $y = f(x)$ when $x f y$ (i.e. $(x,y) \in f$).

Ex: The following are not functions:



1 f a and 1 f b

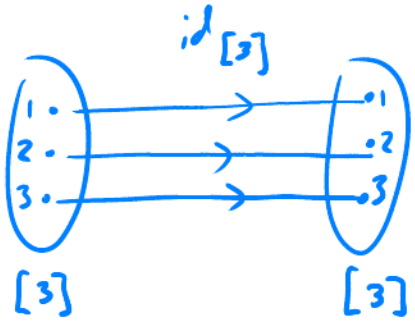


$2 \not f y$ for all $y \in T$.

Point: Every element of dom(f) has exactly one "arrow" leaving it, when f is a function.

Ex: Every set A has a special identity function. $id_A : A \to A$ via $id_A(a) = a$ for all $a \in A$.

↳



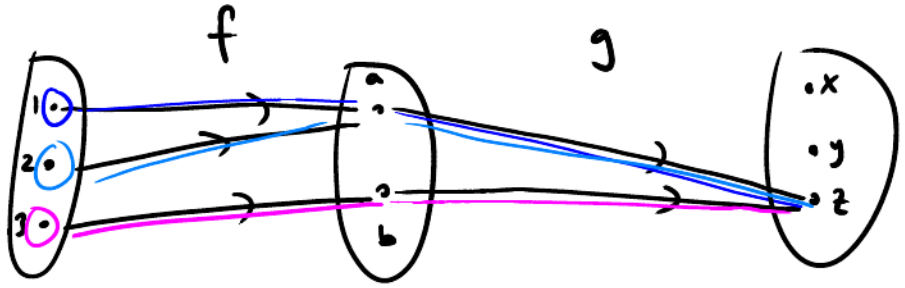
i.e. $id_{[3]} = \{(1,1), (2,2), (3,3)\}$ as a relation on $[3]$.

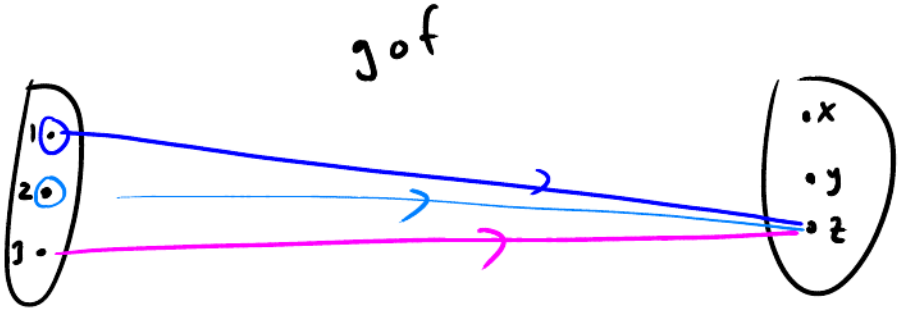
More generally, $id_A = \{(a,a) : a \in A\}$ as a relation ...

Defn: Suppose f, g are functions w/ $\text{cod}(f) = \text{dom}(g)$. The composite of g with f is $g \circ f : \text{dom}(f) \to \text{cod}(g)$ defined by $(g \circ f)(x) = g(f(x))$.

NB: This agrees with the definition from calculus...

Ex: Consider the functions f, g given below:





Ex: Let $f: \mathbb{Z} \to \mathbb{Z}$, $g: \mathbb{Z} \to \mathbb{N}_0$ via $f(x) = 3x+7$ and $g(x) = |x|$. Then the composite $g \circ f: \mathbb{Z} \to \mathbb{N}_0$

$$(g \circ f)(x) = g(f(x)) = g(3x+7) = |3x+7|.$$

On the other hand, $f \circ f: \mathbb{Z} \to \mathbb{Z}$ satisfies

$$(f \circ f)(x) = f(f(x)) = f(3x+7) = 3(3x+7)+7 = 9x+28. \quad \blacksquare$$

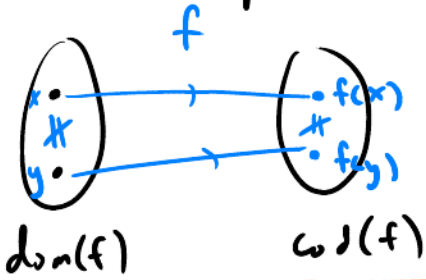
Ex: The function $f: \mathbb{R} \to \mathbb{R}$

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \notin \mathbb{Q} \end{cases}$$

is cool... $\blacksquare$

Defn: A function f is <u>injective</u> (aka <u>into</u> or <u>one-to-one</u>) when for all $x, y \in \text{dom}(f)$ if $f(x) = f(y)$, then $x = y$.

NB: Another, less formal, way to say this is "distinct inputs map to distinct outputs."

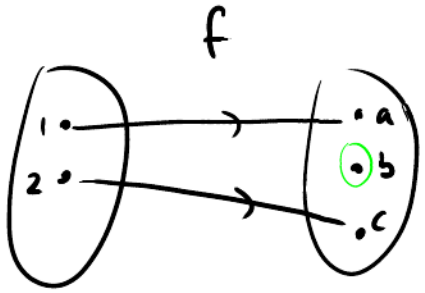


↑ the contrapositive: if $x \neq y$, then $f(x) \neq f(y)$.

Point: f injective: $\forall_{x,y \in dom(f)} [f(x) = f(y) \longrightarrow x = y]$

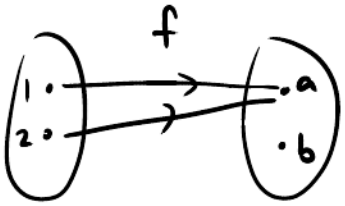
$\equiv \forall_{x,y \in dom(f)} [x \neq y \longrightarrow f(x) \neq f(y)]$

Ex:



is injective.

Ex:



is NOT injective, because $f(1) = a = f(2)$, but $1 \neq 2$.

Ex: The function $f: \mathbb{Z} \to \mathbb{Z}$ w/ $f(x) = 3x + 7$ is injective. Let $x, y \in dom(f) = \mathbb{Z}$ and suppose $f(x) = f(y)$. Hence $3x + 7 = f(x) = f(y) = 3y + 7$, which yields $3x = 3y$ by subtracting 7 and thus $x = y$ by cancelling 3's. Hence $f(x) = f(y)$ implies $x = y$, so f is injective. ☑

NB: $\neg (\forall_{x,y \in dom(f)} [f(x) = f(y) \to x = y])$

$\equiv \exists_{x,y \in dom(f)} (\neg [f(x) = f(y) \to x = y]) \equiv \exists_{x,y \in dom(f)} [f(x) = f(y) \wedge x \neq y]$

Ex: The function $f: \mathbb{Z} \to \mathbb{Z}$ w/ $f(x) = 3x^2$ is not injective. $f(1) = 3 \cdot 1^2 = 3 = 3 \cdot (-1)^2 = f(-1)$, but $1 \neq -1$. ☑